PHISHING AWARENESS & PREVENTION

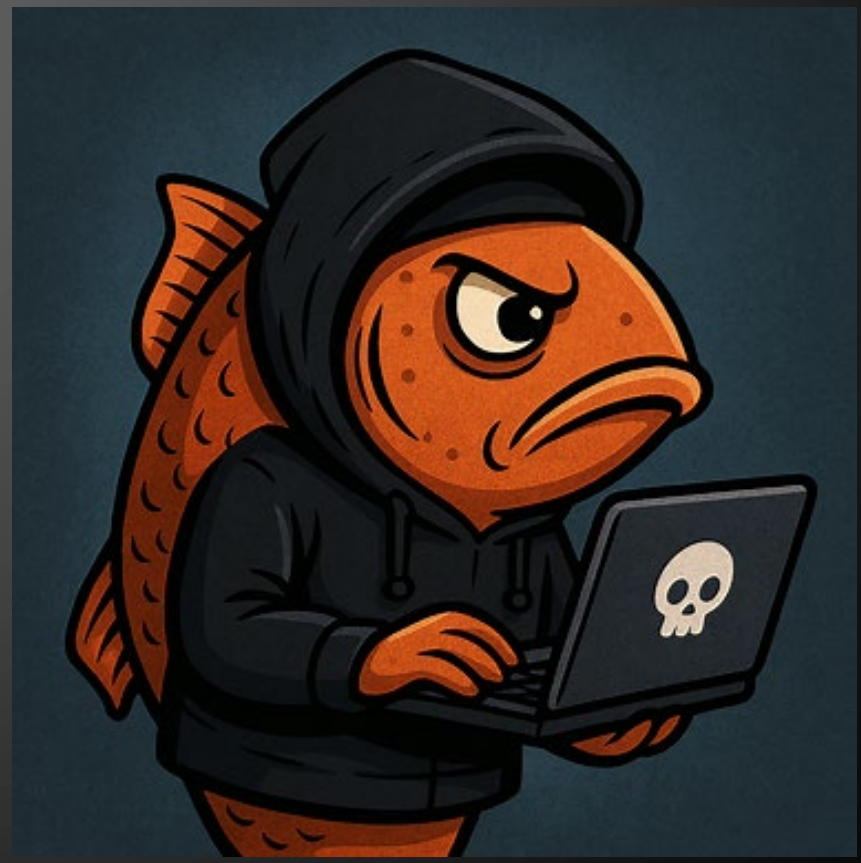
COMMUNITY SERVICES OF NORTHEAST TEXAS

PROTECTING DONORS, STAFF, AND OUR MISSION

BY: CSNT I.T. DEPARTMENT(2026)

WHAT IS PHISHING?

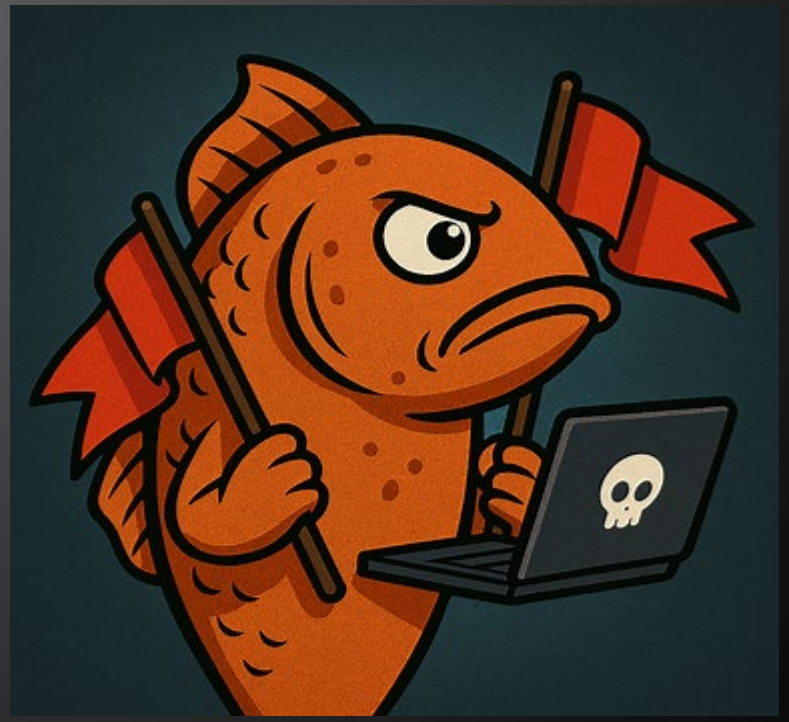
- **DEFINITION:**
  PHISHING = FRAUDULENT EMAILS OR MESSAGES DESIGNED TO TRICK YOU INTO:
- CLICKING MALICIOUS LINKS
- OPENING INFECTED ATTACHMENTS
- SHARING PASSWORDS OR SENSITIVE INFORMATION
- SENDING MONEY OR CHANGING BANKING DETAILS
- WHAT IS PHISHING? LEARN HOW THIS ATTACK WORKS
- **WHY IT MATTERS:**
  NONPROFITS ARE TARGETED BECAUSE WE HANDLE DONOR AND FINANCIAL DATA.



COMMON PHISHING RED FLAGS

- CHECK FOR:
  ✓ SUSPICIOUS SENDER EMAIL (NOT JUST DISPLAY NAME)
  ✓ URGENT LANGUAGE (“ACT NOW!”)
  ✓ REQUESTS FOR PERSONAL INFO OR PASSWORDS
  ✓ UNSOLICITED ATTACHMENTS
  ✓ LINKS THAT DON’T MATCH THE WEBSITE

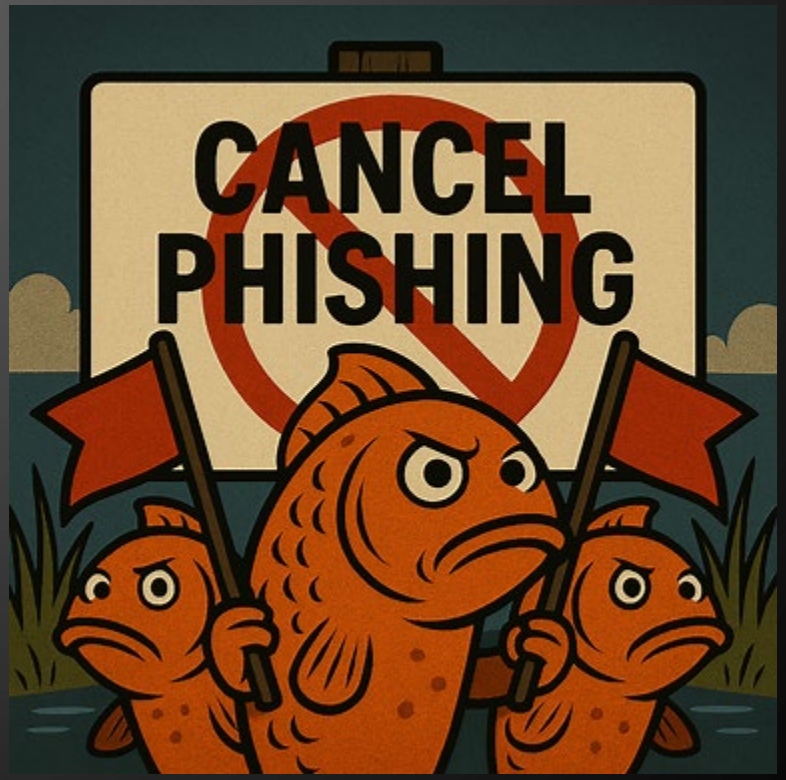
- *RULE OF THUMB:* WHEN IN DOUBT — STOP AND VERIFY.



HOW TO PREVENT PHISHING

1. **NEVER SHARE YOUR PASSWORD**
2. **USE MULTI-FACTOR AUTHENTICATION (MFA)**
3. **HOVER OVER LINKS** TO VERIFY URLS
4. **VERIFY MONEY REQUESTS BY PHONE**
5. **ONLY USE APPROVED ORGANIZATIONAL SYSTEMS**
6. **REPORT SUSPICIOUS EMAILS IMMEDIATELY**

WHAT IS PHISHING? HOW DO I AVOID THE BAIT?



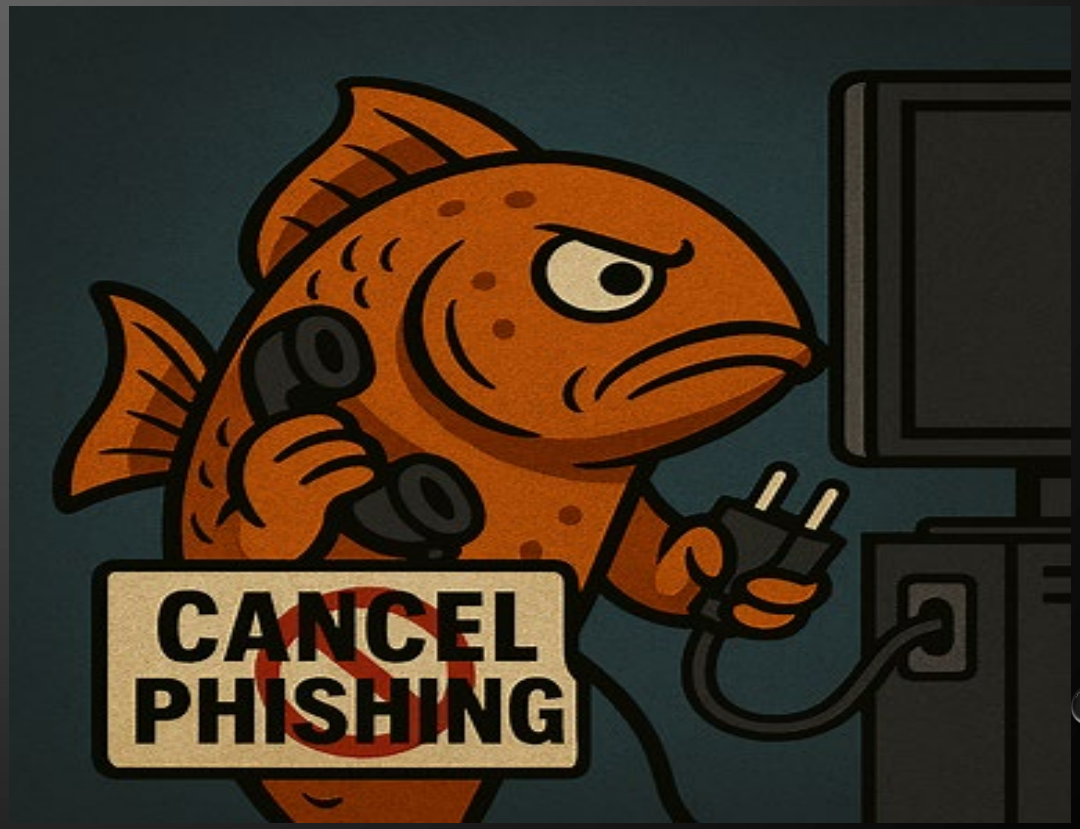
WHAT TO DO IF YOU CLICK

DO NOT PANIC!!!!

IMMEDIATELY:

1. DISCONNECT FROM WI-FI (IF INSTRUCTED)
2. CONTACT IT
3. REPORT THE EMAIL
4. **DO NOT DELETE** EVIDENCE

- FAST REPORTING PREVENTS DAMAGE.



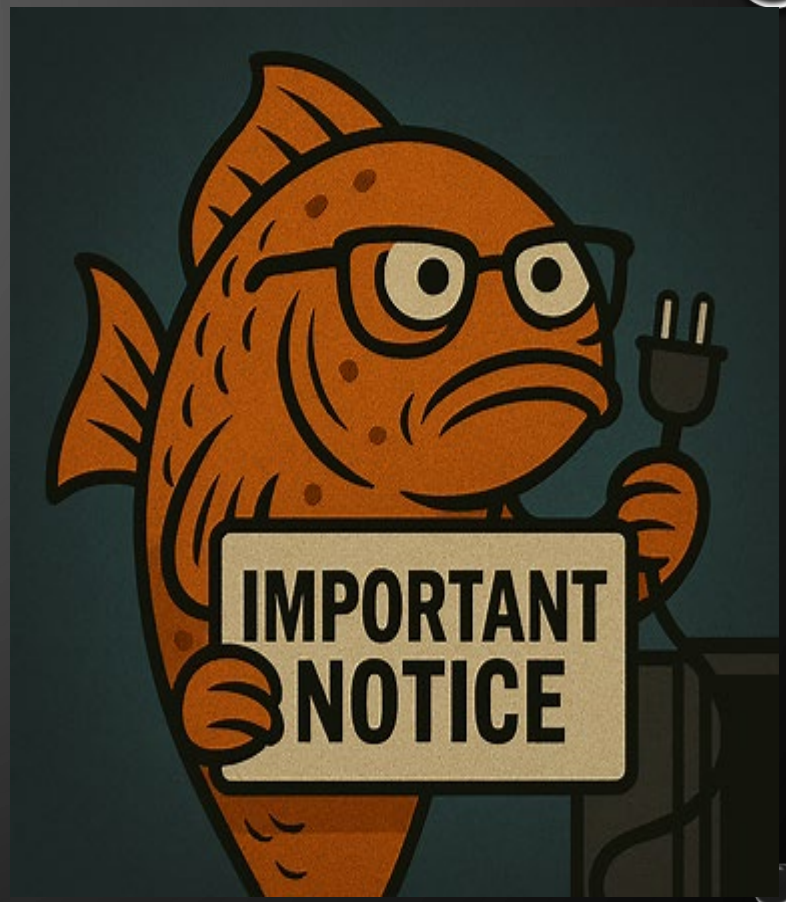
IMPORTANT NOTICE

ALL ORGANIZATION EMAIL AND DEVICES ARE MONITORED FOR SECURITY PURPOSES.

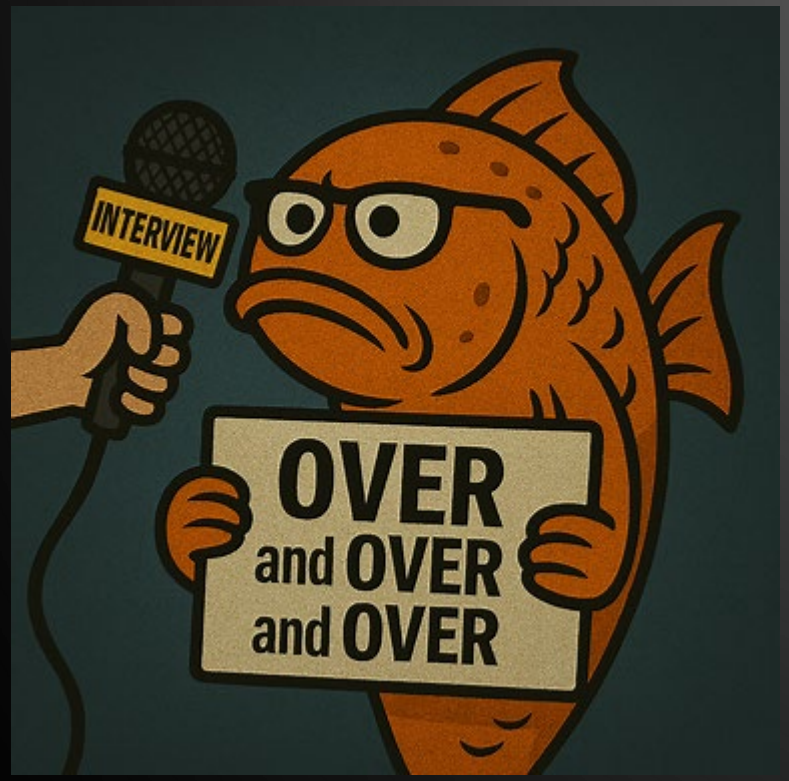
THERE IS NO EXPECTATION OF PRIVACY WHEN USING COMPANY SYSTEMS.

MONITORING HELPS PROTECT:

- DONORS
- FINANCIAL RECORDS
- OUR MISSION



QUIZ / KNOWLEDGE CHECK



- True/False: Always click links in emails from donors.
- What's the first step if you suspect phishing?
- How would you handle an email with invoice request from an "executive"?
- If a failed phishing happens you will have to watch these two videos over & over until you get it right!

- EMAIL SECURITY AWARENESS VIDEO (WHITE BOARD STYLE)
- AVOIDING PHISHING SCAMS: HOW TO SPOT AND PREVENT EMAIL PHISHING ATTACKS

Technology & Cybersecurity Policy

Community Services of Northeast Texas
Effective Date:
Approved By:
Policy Owner: David Buford(CSNT I.T. Department)

1. Purpose
This policy establishes a cybersecurity and technology governance framework to protect:
Donor information
Beneficiary/client data
Financial records
Grant documentation
Staff and volunteer communications
Organizational intellectual property
This policy aligns with the National Institute of Standards and Technology Cybersecurity Framework (CSF) functions: Govern, Identify, Protect, Detect, Respond, and Recover.

2. Scope
This policy applies to:
Employees (full-time and part-time)
Volunteers
Contractors
Board members
Interns
Third-party service providers
All devices accessing organizational systems (including BYOD)

3. Governance (CSF – Govern)
3.1 Cybersecurity Oversight
The Board of Directors provides oversight of cybersecurity risk.
Leadership will:
Review cybersecurity risk annually
Approve major IT expenditures
Review incident reports for significant events

3.2 Risk Management
The organization will:
Conduct annual risk assessments
Identify threats to donor and client data
Document mitigation plans
Track remediation progress

4. Identify (Asset & Risk Management)

4.1 Asset Inventory
IT will maintain an up-to-date inventory of:
Laptops and desktops
Mobile devices
Servers
Cloud applications
Donor management systems
Financial systems
Shared drives
Each asset must have:
Assigned owner
Assigned department
Risk classification

4.2 Data Classification
All data must be classified:

Level	Examples
Public-	Website content, press releases
Internal-	Internal communications
Confidential-	Donor lists, grant applications
Restricted-	Financial records, SSNs, health information

Handling rules:
Confidential and Restricted data must be encrypted in transit.
Restricted data must be encrypted at rest.
Access must be limited to authorized personnel only.

5. Protect (Safeguards & Handling Procedures)
5.1 Acceptable Use of Technology
Technology resources are for organizational purposes.

Users may NOT:
Share login credentials
Download unauthorized software
Access inappropriate or illegal content
Use personal email for organizational business
Connect unauthorized devices to the network
Limited personal use is permitted if it does not interfere with duties or create security risk.

5.2 Access Control
Access is granted based on job role.
Multi-Factor Authentication (MFA) is required for:
Email
Cloud systems

Remote access
Accounts are disabled immediately upon termination.
Access reviews occur quarterly.

5.3 Device Handling Procedures
All Organizational Devices Must:
Use full-disk encryption
Have automatic security updates enabled
Run approved endpoint protection software
Be password protected with auto-lock enabled
Be centrally managed where possible
Lost or Stolen Devices
Must be reported within 1 hour of discovery.

IT will:
Remotely wipe device (if possible)
Disable access credentials
Conduct risk assessment

5.4 Email Use Policy (Mandatory Training Required)

Email is a primary attack vector and must be handled carefully.
Required Training

All staff and volunteers must:
Complete a mandatory email security training video annually
Complete training before system access is granted
Pass a phishing awareness assessment
Training must include:
Identifying phishing emails
Recognizing spoofed senders
Handling suspicious attachments
Avoiding wire fraud scams
Reporting suspicious emails
Email Handling Rules

Users must:
Verify requests involving money transfers
Confirm donor change-of-information requests
Avoid clicking suspicious links
Report suspicious emails immediately using the designated reporting method
Phishing simulations may be conducted periodically.
Failure to complete required training may result in suspension of email access.

5.5 Data Handling Procedures
Confidential and Restricted data:
Must only be stored in approved systems
Must not be stored on personal USB drives
Must not be shared via personal email
Must be shared via secure file-sharing tools
Must be deleted according to retention policy
Printing sensitive data should be minimized.

5.6 Cloud & Vendor Management
Before using any new software or cloud tool:
IT approval is required
A security review must be conducted
Data protection agreements must be in place
Shadow IT is prohibited.

6. Detect (Monitoring & Logging)
6.1 Monitoring Notice
All technology systems, devices, networks, email communications, and internet activity are subject to monitoring.
By using organizational technology resources, users acknowledge:
There is no expectation of privacy
Activity may be logged and reviewed
Security monitoring is continuous
Monitoring may include:
Email scanning
Internet activity logging
Device activity logging
Login tracking
Data transfer monitoring
Monitoring is conducted in accordance with applicable laws.

6.2 Continuous Monitoring
The organization will:
Collect and review security logs
Monitor failed login attempts
Monitor administrative access
Conduct periodic vulnerability scans

7. Respond (Incident Response)
7.1 Reporting Requirements
Users must report:
Suspected phishing
Lost or stolen devices

Data exposure
Malware infections
Suspicious behavior
Reports must be made immediately to IT or the Executive Director.

7.2 Incident Handling Procedures
IT will:
Identify the incident
Contain affected systems
Preserve evidence
Eradicate malicious activity
Restore systems from backups if necessary
Conduct post-incident review

If required, the organization will:
Notify affected donors
Notify regulatory bodies
Notify law enforcement

8. Recover (Business Continuity & Disaster Recovery)
8.1 Backup Policy
Critical systems must:
Be backed up daily (or appropriate frequency)
Use encrypted backups
Maintain offsite or cloud backup
Test recovery procedures annually

8.2 Disaster Recovery
A Disaster Recovery Plan must define:
Recovery Time Objectives (RTO)
Recovery Point Objectives (RPO)
Roles and responsibilities

9. Security Awareness Program
The organization shall maintain:
Annual cybersecurity awareness training
Mandatory email security training video
Periodic phishing simulations
Policy acknowledgment forms
New hires and volunteers must complete training before system access.

10. Policy Violations
Violations may result in:
Revocation of system access

Disciplinary action
Termination
Legal action if applicable

11. Policy Review
This policy shall be reviewed annually by:
Executive Director
IT Lead
Board representative
Acknowledgment Statement
All users must sign an acknowledgment stating they:
Understand this policy
Agree to comply
Understand that technology use is monitored
Understand training is mandatory

Acceptable Use & Technology Monitoring Acknowledgment Form

Community Services of Northeast Texas

I acknowledge that I have received, read, and understand the organization's Technology & Cybersecurity Policy.

By signing below, I agree to the following:

I will use organizational technology resources (including computers, mobile devices, email, internet access, and cloud systems) for authorized business purposes only.

I will protect my login credentials and will not share passwords or accounts with others.

I will comply with all data protection requirements, including safeguarding donor, client, financial, and confidential information.

I will complete all required cybersecurity and email security training, including mandatory annual training and phishing awareness exercises.

I will immediately report:

Suspicious emails or phishing attempts

Lost or stolen devices

Suspected security incidents

Unauthorized access to data

I understand that:

All organizational technology devices, systems, networks, email communications, and internet activity are subject to monitoring.

I have no expectation of privacy when using organizational technology resources.

Activity may be logged, reviewed, and audited in accordance with applicable laws.

I understand that failure to comply with the Technology & Cybersecurity Policy may result in disciplinary action, up to and including termination of employment, volunteer status, or contract.

User Information

Name (Printed): _____

Role/Title: _____

Department: _____

Signature: _____

Date: _____